

WHAT IS CLAIMED IS:

1. A computer-implemented method for multi-level memory domain protection, comprising the steps of:

establishing a domain process context having operating system code, executing at a first protection level, and domain code, executing at a second protection level;

establishing a user process context having the operating system code, executing at the first protection level, and user code, executing at the second protection level; and

protecting the domain code, executing at the second protection level, from the user code, executing at the second protection level, by context switching between the user process context and the domain process context.

2. The method of claim 1, wherein the domain code includes domain-to-user control transfer instructions, the method further comprising the step of transferring control to the user process context in response to the domain-to-user control transfer instructions.

3. The method of claim 1, wherein the user code includes user-to-domain control transfer instructions, the method further comprising the step of transferring control to the domain process context in response to the user-to-domain control transfer instructions.

10 returning to the user code; and
11 resume executing the user code.

1 6. The method of claim 1, further comprising the steps of:
2 executing a portion of the domain code, in the domain process context,
3 calling for execution of targeted user code;
4 branching to a target code-segment corresponding to the targeted user code;
5 executing linking-code in the target code-segment and entering the
6 operating system code in the domain process context;
7 intra-group context switching from the domain process context to the user
8 process context;
9 branching from the operating system code in the user process context to the
10 targeted user code;
11 executing the targeted user code; and
12 returning to the domain code.

1 7. The method of claim 6, wherein the step of returning further comprises the
2 steps of:
3 executing the operating system code, in the user process context, calling for
4 return to the domain code in the domain process context;
5 intra-group context switching from the user process context to the domain
6 process context;
7 entering the target code-segment;

3 means for creating a domain process context, having an operating system
4 code executing within a first protection level, a domain code executing within a
5 second protection level, and a user code residing within the second protection
6 level;

7 means for creating a user process context, having the operating system code
8 executing within the first protection level, a non-executable reserved portion, and
9 the user code executing within the second protection level; and

10 means for protecting the domain code from the user code by locating the
11 domain code in the non-executable reserved portion.

1 16. A computer-useable medium embodying computer-readable program code
2 for causing a computer to perform multi-level memory domain protection by
3 performing the steps of:

4 establishing a domain process context having an operating system code,
5 executing at a first protection level, and a domain code, executing at a second
6 protection level;

7 establishing a user process context having the operating system code,
8 executing at the first protection level, and a user code, executing at the second
9 protection level; and

10 protecting the domain code, executing at the second protection level, from
11 the user code, executing at the second protection level, by context switching
12 between the user process context and the domain process context.

1 17. The computer-useable medium of claim 16, wherein the domain code
 2 includes domain-to-user control transfer instructions, further comprising the step
 3 of transferring control to the user process context in response to the domain-to-
 4 user control transfer instructions.

1 18. The computer-useable medium of claim 16, wherein the user code includes
 2 user-to-domain control transfer instructions, further comprising the step of
 3 transferring control to the domain process context in response to the user-to-
 4 domain control transfer instructions.

1 19. A computer-useable medium embodying computer-readable program code
 2 for causing a computer to perform multi-level memory domain protection by
 3 performing the steps of:
 4 creating a domain process context, having an operating system code
 5 executing within a first protection level, a domain code executing within a second
 6 protection level, and a user code residing within the second protection level;
 7 creating a user process context, having the operating system code executing
 8 within the first protection level, a non-executable reserved portion, and the user
 9 code executing within the second protection level; and
 10 protecting the domain code from the user code by locating the domain code
 11 in the non-executable reserved portion.

1 20. A system for multi-level memory domain protection, the system
2 comprising:
3 a user process, for executing operating system code at a first protection level
4 and for executing user code at a second protection level;
5 a domain process, for executing the operating system code at the first
6 protection level, for executing domain code at the second protection level; and
7 an intra-group context switch, for switching between the user process and the
8 domain process.

1 21. The system of claim 20, wherein the user code includes user-to-domain
2 control transfer instructions, the system further comprising a user call gate,
3 coupled to the user process and the domain process, the user call gate for storing
4 user-to-domain control transfer instructions.

1 22. The system of claim 20, wherein the domain code includes domain-to-user
2 control transfer instructions, the system further comprising a domain call gate,
3 coupled to the user process and the domain process, the domain call gate for
4 storing the domain-to-user control transfer instructions.

1 23. The system of claim 20 further comprising:
2 a second user process, for executing the operating system code at the first
3 protection level and for executing second user code at the second protection level;

4 a second domain process, for executing the operating system code at the first
5 protection level, for executing second domain code at the second protection level;
6 and

7 a inter-group context switch, for switching from the domain process to the
8 second domain process and from the domain process to the second user process.

1 24. The system of claim 21 wherein the user call gate comprises a target code-
2 segment for storing user-to-domain control transfer instructions which transfer
3 control to a specific location in the domain code.

1 25. The system of claim 24 wherein the target code-segment comprises:
2 an address, corresponding to the specific location in the domain code;
3 arguments to be passed from the user process to the domain process; and
4 a data type description of the arguments.

1 26. The system of claim 24 wherein the target code-segment comprises linking-
2 code, for handling how the user-to-domain control transfer instructions are
3 executed.

1 27. The system of claim 24 wherein the target code-segment comprises a calling-
2 code return state, for storing a current state of the user process prior to when one
3 of the user-to-domain instructions is executed.

add A17